3. Ennumeration

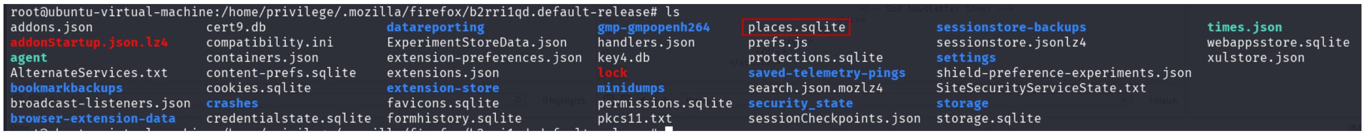
Enumerating the machine gives few leads to move forward. We saw this machine has another adapter as well connected in different networks.

Let’s search for browser history / bookmarks, it has been found that the machine has Mozilla Firefox installed.
`#sudo find / -iname "*firefox*" 2>/dev/null`
``#sudo find / -type d -name "*.default-release" 2>/dev/null

We're going to choose this specific directory `**b2rri1qd.default-release**` because it's the **active Firefox profile directory**: the one Firefox is currently using to store:

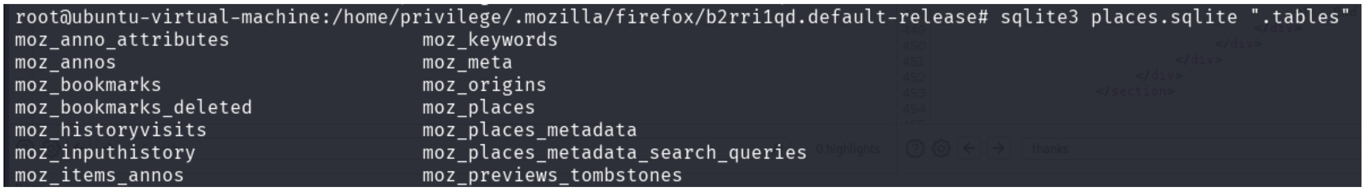
- **Bookmarks**
- **Browsing history**
- **Cookies**
- **Saved logins**
- **Extensions**
- **Preferences**

`# cd /home/privilege/.mozilla/firefox/b2rri1qd.default-release` # ls -lha



```
root@ubuntu-virtual-machine:/home/privilege/.mozilla/firefox/b2rri1qd.default-release# ls
addons.json               cert9.db                 datareporting                gmp-gmpopenh264     places.sqlite            sessionstore-backups                times.json
addonStartup.json.lz4     compatibility.ini        ExperimentStoreData.json     handlers.json       prefs.js                 sessionstore.jsonlz4                webappsstore.sqlite
agent                     containers.json          extension-preferences.json   key4.db             protections.sqlite       settings                            xulstore.json
AlternateServices.txt     content-prefs.sqlite     extensions.json              lock                saved-telemetry-pings    shield-preference-experiments.json
bookmarkbackups           cookies.sqlite           extension-store              minidumps           search.json.mozlz4       SiteSecurityServiceState.txt
broadcast-listeners.json  crashes                  favicons.sqlite              permissions.sqlite  security_state           storage
browser-extension-data    credentialstate.sqlite   formhistory.sqlite           pkcs11.txt          sessionCheckpoints.json  storage.sqlite
```

We will use sqlite3 to access the firefox database as follows

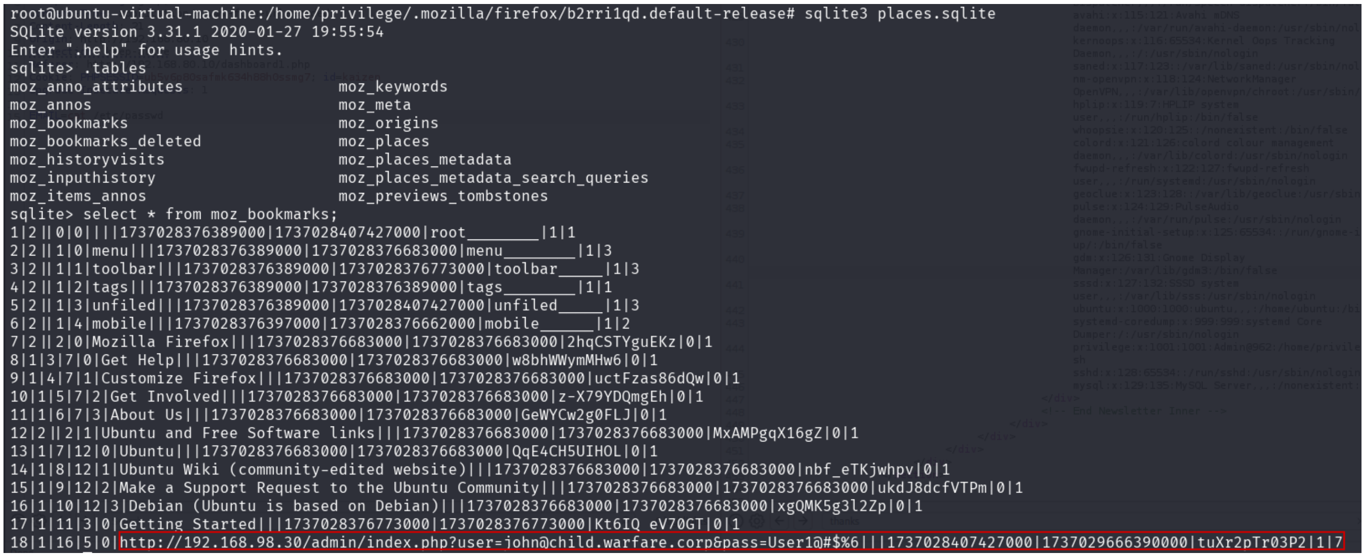


```
root@ubuntu-virtual-machine:/home/privilege/.mozilla/firefox/b2rri1qd.default-release# sqlite3 places.sqlite ".tables"
moz_anno_attributes                 moz_keywords
moz_annos                           moz_meta
moz_bookmarks                       moz_origins
moz_bookmarks_deleted               moz_places
moz_historyvisits                   moz_places_metadata
moz_inputhistory                    moz_places_metadata_search_queries
moz_items_annos                     moz_previews_tombstones
```

We specifically chose the `places.sqlite` file because it is **the central Firefox database that stores both:

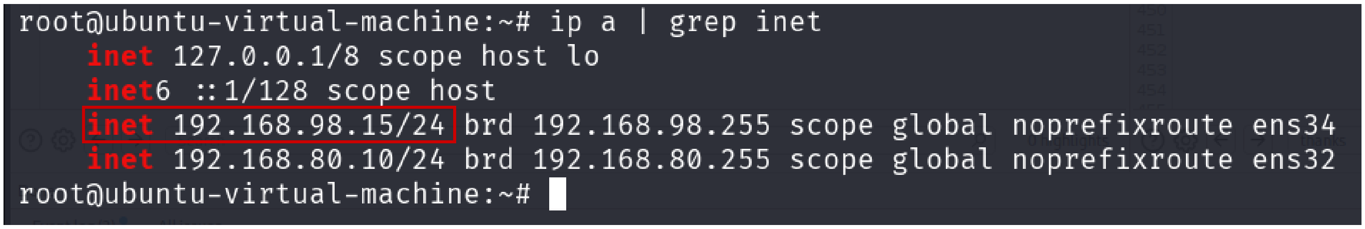
- **Bookmarks**
- **Browsing history**

```
#sqlite3 places.sqlite
sqlite> .tables
sqlite> select * from moz_bookmarks;
```



```
root@ubuntu-virtual-machine:/home/privilege/.mozilla/firefox/b2rri1qd.default-release# sqlite3 places.sqlite
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> .tables
moz_anno_attributes                 moz_keywords
moz_annos                           moz_meta
moz_bookmarks                       moz_origins
moz_bookmarks_deleted               moz_places
moz_historyvisits                   moz_places_metadata
moz_inputhistory                    moz_places_metadata_search_queries
moz_items_annos                     moz_previews_tombstones
sqlite> select * from moz_bookmarks;
1|2||0|0||||1737028376389000|1737028407427000|root________|1|1
2|2||1|0|menu|||1737028376389000|1737028376683000|menu________|1|3
3|2||1|1|toolbar|||1737028376389000|1737028376773000|toolbar_____|1|3
4|2||1|2|tags|||1737028376389000|1737028376389000|tags________|1|1
5|2||1|3|unfiled|||1737028376389000|1737028407427000|unfiled_____|1|3
6|2||1|4|mobile|||1737028376397000|1737028376662000|mobile______|1|2
7|2||2|0|Mozilla Firefox|||1737028376683000|1737028376683000|2hqCSTYguEKz|0|1
8|1|3|7|0|Get Help|||1737028376683000|1737028376683000|w8bhWWymMHw6|0|1
9|1|4|7|1|Customize Firefox|||1737028376683000|1737028376683000|uctFzas86dQw|0|1
10|1|5|7|2|Get Involved|||1737028376683000|1737028376683000|z-X79YDQmgEh|0|1
11|1|6|7|3|About Us|||1737028376683000|1737028376683000|GeWYCw2g0FLJ|0|1
12|2||2|1|Ubuntu and Free Software links|||1737028376683000|1737028376683000|MxAMPgqX16gZ|0|1
13|1|7|12|0|Ubuntu|||1737028376683000|1737028376683000|QqE4CH5UIHOL|0|1
14|1|8|12|1|Ubuntu Wiki (community-edited website)|||1737028376683000|1737028376683000|nbf_eTKjwhpv|0|1
15|1|9|12|2|Make a Support Request to the Ubuntu Community|||1737028376683000|1737028376683000|ukdJ8dcfVTPm|0|1
16|1|10|12|3|Debian (Ubuntu is based on Debian)|||1737028376683000|1737028376683000|xgQMK5g3l2Zp|0|1
17|1|11|3|0|Getting Started|||1737028376773000|1737028376773000|Kt6IQ eV70GT|0|1
18|1|16|5|0|http://192.168.98.30/admin/index.php?user=john@child.warfare.corp&pass=User1@#$%6|||1737028407427000|1737029666390000|tuXr2pTr03P2|1|7
```

--> We found some interesting credentials in the mozilla bookmarks database, divulgating a new network segment: 192.168.98.0/24



```
root@ubuntu-virtual-machine:~# ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 192.168.98.15/24 brd 192.168.98.255 scope global noprefixroute ens34
    inet 192.168.80.10/24 brd 192.168.80.255 scope global noprefixroute ens32
root@ubuntu-virtual-machine:~#
```

--> We have to perform pivoting as 192.168.98.0/24 is not directly accessible from the VPN network. We will utilize **ligolo-ng** for the same.